Extension to DTLS
Securing Multicast Group Communication

DTLS-based Multicast Security for Low-Power and Lossy Networks (LLNs)

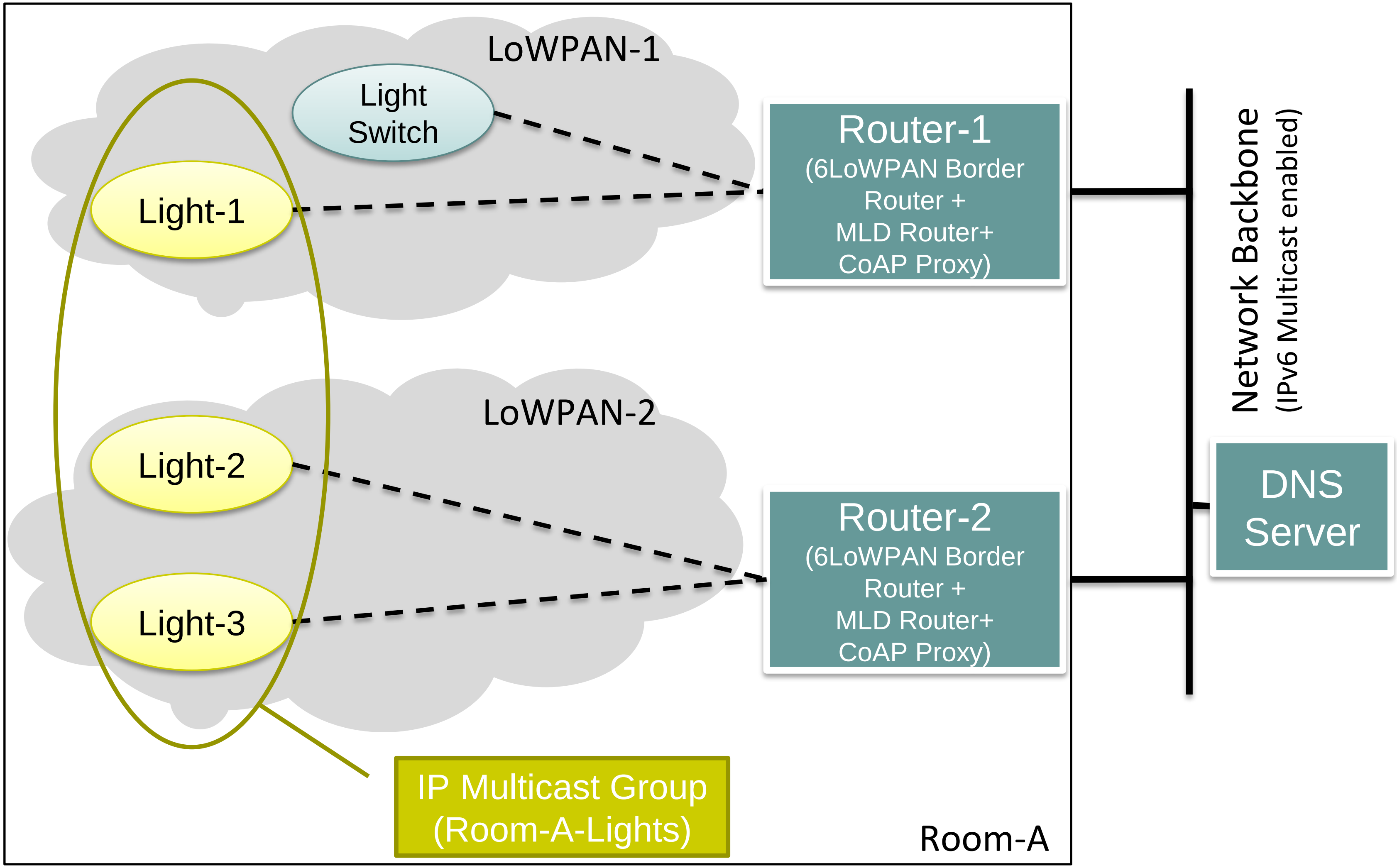
draft-keoh-tls-multicast-security

***Sye Loong Keoh**, Oscar Garcia-Morchon, Sandeep S. Kumar, Esko Dijk*

IETF85 Nov 4 – 9, 2012, Atlanta

Email: sye.loong.keoh AT philips.com

Group Communication Use Cases


LoWPAN-1
Light Switch
Light-1
Router-1 (6LoWPAN Border Router + MLD Router+ CoAP Proxy)
Network Backbone (IPv6 Multicast enabled)
LoWPAN-2
Light-2
Light-3
DNS Server
Router-2 (6LoWPAN Border Router + MLD Router+ CoAP Proxy)
IP Multicast Group (Room-A-Lights)
Room-A

Source: Group Communication for CoAP (draft-ietf-core-groupcomm)

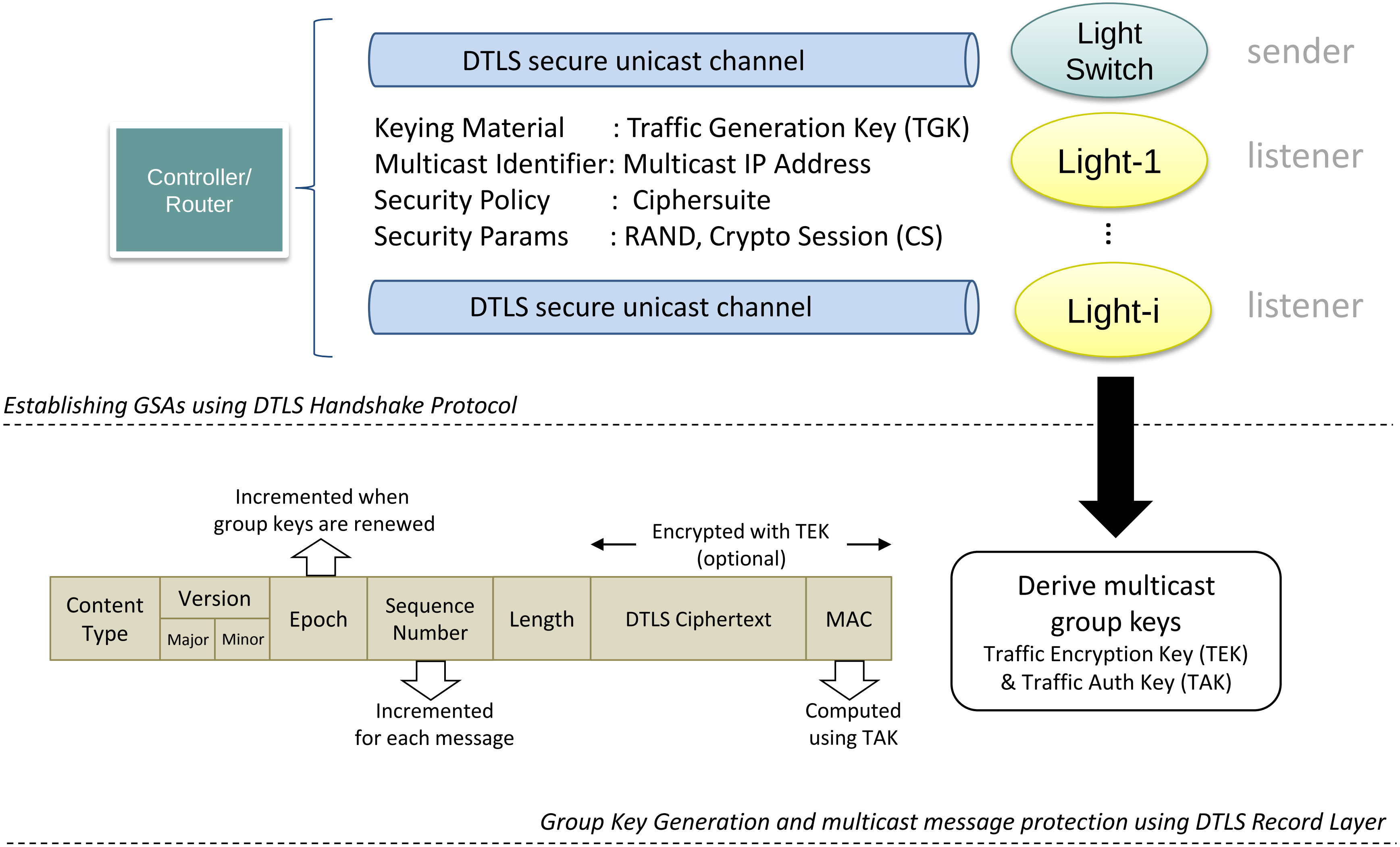
Motivation & Requirements

- **Group communication (in LLNs):** also vulnerable to eavesdropping, tampering, message forgery, replay, etc.
- **Limited resource and memory:** reduce the number of cryptographic protocols, reuse security protocol.
- **DTLS is must-implement for CoAP:** IPSec is optional, extend DTLS to secure multicast group communication.

Requirements

- A Group Security Association (GSA): *distribute keying materials*.
- Multicast security policy: *specify the ciphersuite for encryption and authentication.*
- Multicast key management: *update/renew group keys periodically.*
- Group level data integrity and authentication
- Data source authentication (out-of-scope)
- Data confidentiality (optional)
- Replay protection

Overview of DTLS Multicast Security



Controller/ Router

DTLS secure unicast channel

Keying Material	: Traffic Generation Key (TGK)
Multicast Identifier	: Multicast IP Address
Security Policy	: Ciphersuite
Security Params	: RAND, Crypto Session (CS)

DTLS secure unicast channel

Light Switch	sender
Light-1	listener
⋮	
Light-i	listener

Establishing GSAs using DTLS Handshake Protocol

Incremented when group keys are renewed

Encrypted with TEK (optional)

Content Type	Version Major / Minor	Epoch	Sequence Number	Length	DTLS Ciphertext	MAC

Incremented for each message

Computed using TAK

Derive multicast group keys
Traffic Encryption Key (TEK)
& Traffic Auth Key (TAK)

Group Key Generation and multicast message protection using DTLS Record Layer

Group Keys Generation

- Each device generates Multicast Traffic Encryption Key (TEK) and Traffic Authentication Key (TAK).
- Based on the PRF and P-Function defined in MIKEY [RFC3830]. Use SHA-256 instead of SHA-1.

INKEY : TGK
Inkey_len : bit length of TGK (128-bit)
Label : constant || mul_id || cs_id || RAND
Outkey_len : bit length of output key (128-bit)

- The constant value for TEK: 0x2AD01C64
  For TAK, the constant value is: 0x1B5C7973

Protecting Multicast Messages (1)

- Application message (e.g., CoAP message) is encrypted using TEK, and a MAC is generated using the TAK according to the ciphersuite defined.
- Sequence Number is incremented whenever the sender sends a multicast message.
- All listeners keep track of the sequence number/epoch received to ensure message freshness.

Ciphersuite MTS_WITH_AES_128_CCM_8

- AES CCM mode of operation is an authenticated encryption scheme. Only the TEK is used to encrypt and compute MAC.

Ciphersuite MTS_WITH_NULL_SHA256

- Message is NOT encrypted, hence TEK is not used.
- Message MAC must be computed using the TAK using SHA256.

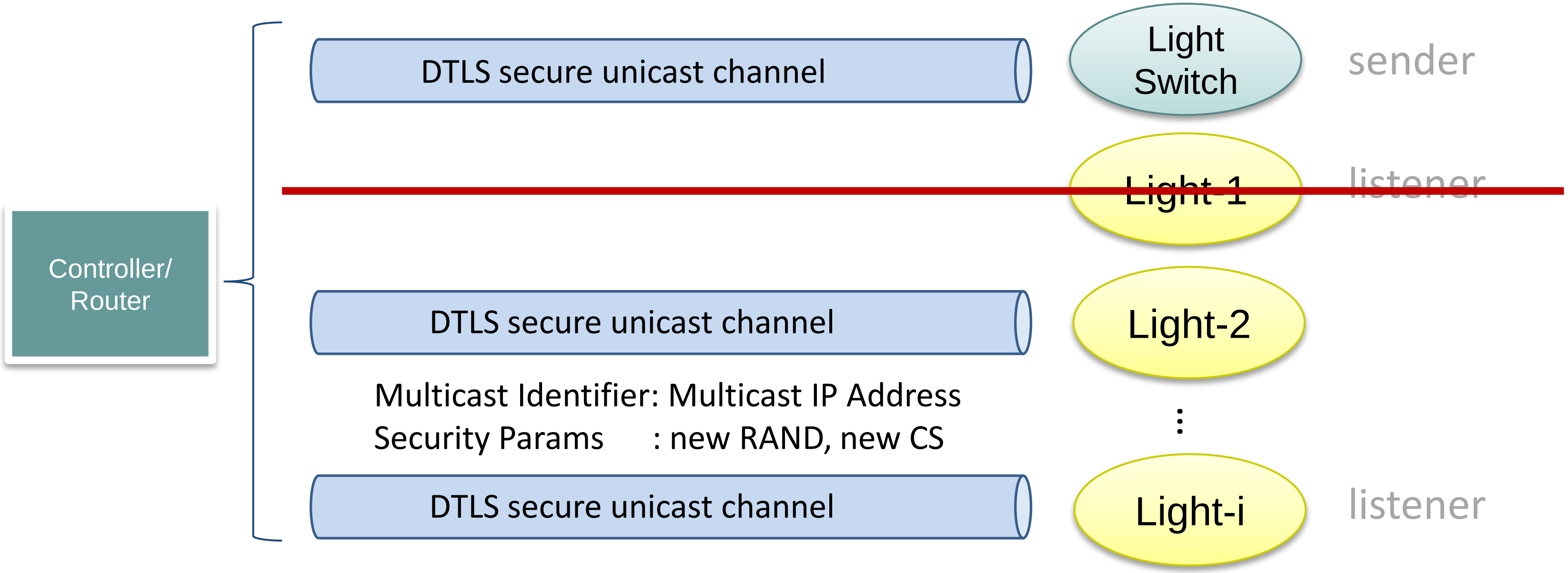
**Define additional ciphersuites that use both TEK and TAK in the future.*

Protecting Multicast Messages (2)

- When receiving a multicast message, devices use the multicast IP address to locate the crypto session in order to obtain the TEK and TAK.
- Use the last received epoch and sequence number to detect message replay.
    - Drop messages that have a sequence number less than or equal to the value stored in the crypto session.
    - Epoch number must match the epoch number stored in the crypto session.

This replay detection mechanism only works on one-to-many communication topology

Group Key Renewal


DTLS secure unicast channel
Light Switch
sender
~~Light-1~~
~~listener~~
Controller/ Router
DTLS secure unicast channel
Light-2
Multicast Identifier: Multicast IP Address
Security Params : new RAND, new CS
⋮
DTLS secure unicast channel
Light-i
listener

Send new security parameters via the DTLS secure channel

- Group keys can be renewed periodically according to a schedule.
- Rely on the DTLS secure channel with each member device to convey new security parameters.
- The 'master key' – i.e., TGK remains the same.

Conclusions

- Group communication is of key importance in machine-to-machine (M2M) applications.
- Propose an extension to DTLS to support secure multicast group communication, need to further specify the DTLS header extension.
- Re-use existing security protocol on constrained devices in LLNs.
- Current proposal only applies to One-to-Many communication topology.